Information Security Statement by
Steven Cooper
Chief Information Officer
U.S. Department of Homeland Security
Before the
U.S. House of Representatives Committee on Government Reform

Thursday, April 7, 2005

Mr. Chairman and Members of the Committee:

Good morning, I am Steve Cooper, Chief Information Officer for the Department of Homeland Security (DHS). It is my pleasure to appear before the Committee and I wish to thank the Chairman and Members for the providing me the opportunity to update you on our efforts and progress in integrating and securing information systems within the Department.

I would like to begin by acknowledging the important role our Inspector General (IG) plays in the Department, and especially with respect to the development and operations of information technologies in support of our mission. The IG has been an important and independent voice as the Department formulates a strategy for building a robust and effective Information Security Program. Mr. Coleman has provided what I believe to be an accurate and detailed assessment of our progress to date, and rather than repeat what has already been said, I would like to focus my remarks on the future.

The DHS Information Security Program is structured around compliance with the Federal Information Security Management Act (FISMA), as well as Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance. Our primary focus is to enable effective and secure information sharing. I want to stress that we are not proud of our failing grade. We have done much, and much needs to be done. Specifically, we have implemented and continue to implement a number of security performance metrics to address the issues brought up in the FISMA grade.

I fully understand that the success of the Department is dependent on our ability to protect sensitive information used to secure the homeland; and, to this end, the Department's Information Security Program has been designed to provide a secure and trusted computing environment based on sound, risk-management principles and program planning. The development of a formal trust model within this Program will eliminate institutional barriers that regularly divide organizations, and will enable disparate agencies to more effectively share information within a common trusted framework. We have implemented a Digital Dashboard that provides the status of security performance based on computed FISMA metrics and we have implemented a security performance scorecard.

Three key Information Security Program initiatives, underway for over a year, are now

providing tangible results. As these three efforts converge, together they will pave the way for real and measurable security improvements in the near future. These include:

(1) Completing a comprehensive base-line inventory for defining accreditation boundaries and assigning responsibilities for security controls to appropriate Program Officials throughout the Department,

(2) Fielding a robust set of automated enterprise security-management tools to optimize our security processes; and,

(3) Implementing a comprehensive and repeatable set of metrics for holding Program Officials accountable.

The base-line systems inventory project now underway has already identified a significant number of legacy systems that were not previously included in the initial system inventory developed during the standup of the Department. At one of the Organizational Elements, the system inventory project has now identified 106 information systems compared to the five systems that were previously identified at stand-up.

In response to this legacy issue, the Department is developing a comprehensive remediation plan for completing all the required Certification and Accreditations (C&As) by the end of fiscal year 2006. Related to these actions, DHS has implemented a Department POA&M [Plan of Action and Milestones] process and an enterprise system to manage the DHS POA&M. Evidence that DHS is successfully institutionalizing the POA&M process is demonstrated by the fact that our initial FY03 POA&M contained less that 100 line items while our current POA&M contains several thousand line items.

Furthermore, DHS has implemented a Certification and Accreditation or C&A tool that will ensure C&A quality and map the C&A testing to the DHS policy. The C&A remediation plan will include a prioritized list of systems to be certified based on the system's security impact level (i.e., systems with high security impact levels will be the first systems to be accredited). The C&A remediation plan will identify a variety of funding alternatives for completing the C&As, our new automated security management tools are already designed to streamline the process. Use of this tool has been mandated for all C&A activity initiated after April 10.

This aggressive remediation effort will provide a sound baseline of secure systems with appropriate controls in place; however, we must continue to improve our security posture throughout the lifecycle of each and every system or application in use in the Department. For this reason, we are continuing to refine the Program so that it will remain relevant for the future. Program enhancements currently underway include:

- Developing a Communications Plan for the DHS Information Security Program, to include an Information Security Portal that will improve the availability of information security data to DHS employees who do not have access to DHS Online.

- Publishing an updated Information Security Program Strategic Plan outlining a revised vision for the future of the program based on lessons learned over the past two years.

Finally, to sustain a viable and healthy Information Security Program, I know that we must have strong support throughout the Department. Through the DHS Chief Information Officers' Council, I will work with each member to ensure that we not only continue to improve our security posture through periodic Program reviews, but that we also implement new and improved measures wherever appropriate. Thank you and I look forward to your questions.